COMBINED FEDERATED BATTLE LABORATORIES NETWORK (CFBLNet)

PUBLICATION 1
ANNEX D

NETWORK OPERATIONS
(Network/System Aspects of CFBLNet)

Version 7.0
September 2012

DOCUMENT CONTROL AND TRACKING METADATA

Security Classification	Unclassified
Access Status	Version 7.0
Usage Condition	Publicly Releasable

Scheme Type	CFBLNet Documentation Control and Tracking Scheme
Scheme Name	See Pub 1, Annex G, CFBLNet Document Management
Title Words	CFBLNet Pub 1 – Annex D, CFBLNet Security and Information Assurance Strategy

Function Descriptor	Network Operations (Network/Systems Aspects of CFBLNet)
Activity Descriptor	Implementation and Guidance

Event Date	**Agent Type**	**Agent Name**	**Agent Details**	**Event Type**	**Event Description**
30Oct09	C-EG	Steve Pitcher	C-EG Chair	Review/Approve Sign	Publication 1, Annex D, Version 6.0
05Sep12	C-EG	Steve Pitcher	C-EG Chair	Review/Approve Sign	Publication 1, Annex D, Version 7.0

TABLE OF CONTENTS

APPENDIX 1 -- CFBLNET LEVEL 0 TOPOLOGY

APPENDIX 2 -- BLACK IP ADDRESS SPACE ALLOCATION

APPENDIX 3 -- CFBLNET VOIP PHONE NUMBER RANGES

CHAPTER 1 - INTRODUCTION

Purpose

101. Annex D to the CFBLNet Publication 1 contains the network operations and system management policies and procedures, related to the operations of the CFBLNet, which functions under the authority of the CFBLNet Technical Arrangement / Charter. It comprises a main body and a range of appendices. Appendices that may not be visible have been deemed to be of a sensitive nature and are available only in a classified controlled version.

Authority

102. CFBLNet Pub 1 Annex D is issued by the CFBLNet Executive Group (C-EG) on behalf of the CFBLNet Senior Steering Group (C-SSG). The provisions of this and all associated publications shall govern the conduct of all network activities performed by the CFBLNet participants, subject to their respective Nation’s laws and military regulations.

103. The Network Working Group (NWG) is the technical body, comprised of appropriate experts from the Mission Partners (CMP/GMPs), which supports the network governance process for the CFBLNet on behalf of the C-EG. The terms of reference and responsibilities of the NWG are described within Annex A.

Amendments

104. CFBLNet Pub 1 Annex D may be amended when the NWG determines that there is an identified requirement. The NWG Chair will propose the text of the amendment to the NWG members for endorsement. Once the NWG members have endorsed the amendment, it will be submitted for C-EG approval. Upon approval by the C-EG, the Secretariat will re-issue a new version of Annex D.

Effective Date

105. The current version of CFBLNet Pub 1, Annex D is effective upon the latest approval by the C-EG.

CHAPTER 2 - NETWORK OVERVIEW DESCRIPTION

Infrastructure

201. The CFBLNet infrastructure is a closed, wide area communications network linking CMP/GMP infrastructures, collectively forming the CFBLNet. The CFBLNet Level 0 Topology is illustrated in Appendix 1 of this document. The NWG representatives are responsible for maintaining the individual CMP/GMP Level 1 and Level 2 topology diagrams with the requisite detailed information.

202. The CFBLNet consists of the following components:

a. Black backbone (Blackbone). A common, closed, unclassified IP routed network layer implemented using a mixture of both ATM and IP bearer networks. Its primary purpose is to transport encrypted traffic throughout the network. The level and type of network services available within this component will be the minimal required to support the interconnection of multiple enclaves as agreed to by all CMP/GMPs; see Chapter 5, Table D-5.1 of this document

b. Persistent CFBLNet Enclaves:

i. CFBLNet Unclassified Enclave (CUE). A permanent IP enclave operating over the Blackbone. It will operate at the Unclassified, Non Releasable to Internet, Releasable to CMP/GMPs and to Guest Mission Partners (GMPs) level, as directed by the C-EG. The CUE will be encrypted using Advanced Encryption Standard (AES) algorithms at minimum.

c. Persistent Limited-Audience Enclaves:

i. Four Eyes Enclave. A permanent classified IP network operating over the Blackbone at the SECRET level, releasable to AUS, CAN, UK, US only.

ii. NATO Red Enclave. A permanent classified IP network operating over the Blackbone at the SECRET level, releasable to NATO only.

d. Initiative Enclaves. These are created for a finite period to support the execution of specific Initiatives and operate over the Blackbone Initiative enclaves will be stood up and shut down as required. The level of classification and release caveats used within these enclaves will be determined by the initiative requirements. The coordination and provision of all network services within a specific Initiative enclave will be the responsibility of the Initiative sponsor, unless otherwise agreed.

e. Enclaves will operate Internet Protocol version 4 (IPv4), version 6 (IPv6) or a dual-stack IPv4/IPv6 configuration.

203. Operational control of all network devices must conform to the CFBLNet Pub 1 requirements. CMP/GMPs are responsible for providing connectivity between their national sites and an agreed upon national/organizational Point of Presence (POP) which will serve as their connection point to the CFBLNet. See paragraph 206.

204. Initiative Participants can establish connectivity via any accredited means in accordance with CFBLNet Pub 1 Annex C.

CFBLNet Sites

205. CFBLNet sites are those operational participant sites accredited through the CFBLNet security process (CFBLNet Pub 1 Annex C) and approved by the C-EG. Each NWG member will provide an up-to-date list of new/existing sites on his/her national WAN at each CMM for informational purposes. This list does not need to include individual national/organizational Initiative sites as this is the Nation's prerogative. The NWG is not part of the site approval process.

206. National/Organizational Point Of Presence. A CFBLNet national/organizational POP is a CFBLNet site that provides a point of connectivity between different national/organizational management and administrative domains. The establishment of a peering relationship between two POPs is arranged with the consent of the CMP/GMPs involved.

Cryptographic Services (See also Pub 1 Annex C)

207. Cryptographic Support. The Multinational Information Sharing Program Management Office (MNIS PMO) is responsible for the coordination of cryptographic services for the permanent components of the CFBLNet from the USA sites to National POP sites. Behind the National POP of a given CMP/GMP, that CMP/GMP will be responsible for coordinating their cryptographic services and will provide this information to the NWG. Each CMP/GMP may provide their own cryptographic support for their respective information and administrative domains or arrange other support accordingly. Initiative Sponsors that require special cryptographic services are to coordinate support through their respective CLR.

208. Encryption Devices. CFBLNet enclaves are protected by appropriate and approved encryption devices and border protection systems (BPS) accredited by CMP/GMPs for the protection, as required, of information up to and including the classification level of the enclave.

209. Keying Material (Keymat). Refer to Annex C.

CHAPTER 3 - MANAGEMENT ASPECTS

Introduction

301. This chapter addresses the management requirements of the CFBLNet and is intended to provide a basic understanding of the network operations and the relationship between the CMP/GMPs' management cells.

Management Strategy

302. Each CFBLNet CMP/GMP provides, manages, supports and is responsible for their nation / Organisation infrastructure, which collectively forms the CFBLNet. The MNIS PMO is recognised by the CMP/GMPs as the central body responsible for coordinating the CFBLNet management policies as defined in this Annex.

303. The CFBLNet is a 24x7-accessible network. The USA Combined Communications Control Centre (CCCC), located in Arlington, Virginia, USA is staffed appropriately to support this effort. Initiative Participant manning is based on the requirements dictated by approved CFBLNet Initiatives.

MNIS PMO

304. The MNIS PMO operates and maintains the CCCC and provides the CFBLNet Secretariat resources that coordinate the use of the CFBLNet for Initiatives. The MNIS PMO is responsible for all POP connections within and to the USA WAN infrastructure. The CCCC manages and monitors CFBLNet activities and makes any pertinent information available to the CMP/GMPs during normal operating hours (16x5). The CCCC will provide extended support as required for a specific initiative as defined in the Memorandum of Agreement/Service Level Agreement (MOA/SLA).

NATO C3 Agency

305. The NC3A operates and maintains the European regional POP for NATO nations, NATO organizations and Guest Mission Partners (GMPs) and also provides the cryptographic bridging between NATO, CCEB and USA environments and sponsored nations and organizations, as required.

306. The NC3A also provides administrative support for NATO nations and NATO-sponsored GMPs.

Incident Management

307. The CMP and GMPs are responsible to advise the Secretariat of any CFBLNet activity that is not in compliance with CFBLNet policies and practices. Incidents reported to the Secretariat will be resolved through dialogue with the CMP/GMPs involved. If the situation cannot be resolved, then recommendations will be made to the C-EG for resolution.

Network Documentation

308. Each CMP/GMP will maintain their own detailed network documentation. *

309. There are three levels of documentation that will comply with the security classification appendix within CFBLNet Pub 1 Annex C and are not intended to conflict with CMP/GMP information security/disclosure policies:

a. Level 0. Basic CFBLNet WAN layout drawings showing major components and generic architecture at a level detailing the national Participants and the connectivity attributes between them. (Section 1: Intra-national topology; Section 2: Enclave topology; Section 3: Cryptographic topology; Section 4: Blackbone architecture);

b. Level 1. Detailed CMP/GMP layout drawings, showing major components and generic architecture within a CMP or GMP's domain (Section 1: Topology diagram; Section 2: Enclave matrix; Section 3: Cryptographic plan per site/enclave; Section 4: Blackbone); and

c. Level 2. Detailed site layout drawings, showing IP Addresses, Host Names, cards/ports, hardware/software, versions/revisions, etc. *

* Each nation may share details with relevant countries according to national security standards.

Documentation Guidelines

310. Microsoft Visio, Excel and PowerPoint are the preferred documentation tools. Where possible, documentation should be distributed to the NWG with the capability to drill down to network information where appropriate.

CHAPTER 4 - NETWORK SERVICES OVERVIEW

General

401. Each CMP/GMP maintains and operates agreed levels and types of network services for the CFBLNet permanent components in order to facilitate Initiatives. These network services inter-operate with other CMP/GMPs' services to provide a collective network community. The operation of permanent network services will be coordinated by the CCCC with each CMP/GMP's designated Network Operations Centre (NOC).

Core Network Services

402. Core network services are robust, reliable and stable services, which have been developed and deployed on the CFBLNet permanent components to support Initiatives. They are managed and supported directly by the CMP/GMPs. They are further divided into the following two categories:

a. Critical Infrastructure. Those services that each CMP/GMP is obligated to stand up and support, as part of their minimum network infrastructure, for effective and efficient network operations; and

b. Supporting Infrastructure. Those services that provide a value added benefit but which are not essential for effective network operations and can be hosted by any CMP/GMP on behalf of other CMP/GMPs.

403. The NWG provides recommendations to the C-EG on what core network services will be deployed on the CFBLNet Persistent Enclaves, its category and operational status in light of anticipated activities. It is the responsibility of the Initiative Sponsors to determine and support any network services that are required within an Initiative as these will be deemed separate from the CFBLNet Core Network Services.

404. An Initiative may deploy additional network services required to support activities specific to that Initiative. As part of the review of Initiative activities, the NWG will consider these additional network services for inclusion as part of the CFBLNet core network services for some or all of the CFBLNet permanent components. This process is managed by the NWG and follows the method illustrated in Figure D-4.1.

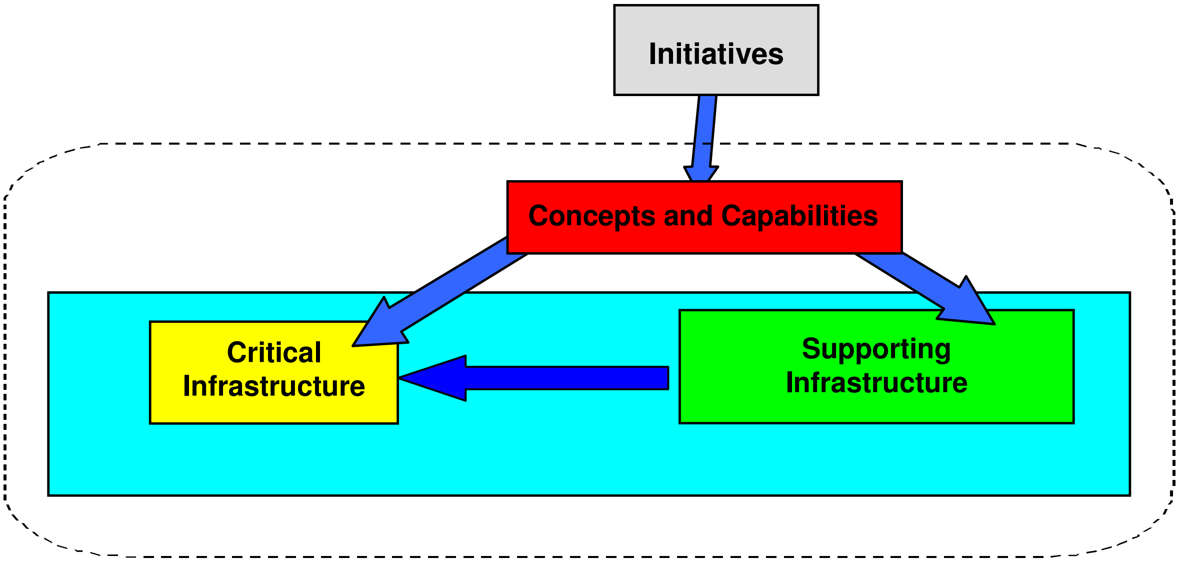

Figure D-4.1, CFBLNet Network Services

Internet Protocol (IP) Address Space

405. CMP/GMPs are responsible for managing their own IP address space to support their network infrastructure requirements. IP address spaces are allocated through the NWG.

406. CMP/GMPs will use an agreed upon IP address space for the CFBLNet persistent enclaves (detailed in Appendix 2), thus minimizing the possibility of address space conflict. The CCCC is responsible for maintaining a register of all CFBLNet IP address spaces.

407. CFBLNet Initiatives, utilizing the persistent enclaves, will coordinate with their respective NWG representative to obtain IP space allocations. For those Initiatives utilizing a separate temporary enclave, NWG representatives will recommend the IP address space allocation for use within the enclave.

408. The NWG is responsible for the assignment of Border Gateway Protocol (BGP) Autonomous System (AS) numbers to each CMP/GMP.

CHAPTER 5 - CFBLNet BLACKBONE

General

501. The purpose of the Blackbone is to provide a permanent, common, closed, unclassified transport (bearer) layer. Its primary function is to transport encrypted traffic throughout the network. There are no network services available within this component, except those required for engineering purposes, as agreed by the NWG.

502. The core network services for the Blackbone are depicted in Table D-5.1.

Ser (a)	Information Service Description (b)	Status (c)
1	Internet Protocol version 4 (IPv4)	Required
2	Network Service Access Point Addressing	Required
3	Routing Protocols (e.g., BGP)	Required
4	Network Time Protocol (NTP)	Required
5	Internet Protocol version 6 (IPv6)	Available
6	IP Multicasting	Available
7	Bandwidth Management	Available
8	VOIP	Available

Table D-5.1, IPv4 Blackbone Core Network Services

Routing Protocols

503. The primary routing protocol used on the CFBLNet Blackbone will be Border Gateway Protocol (BGP). Choice of routing protocol for CMP/GMP internal distribution of routes will be at the discretion of each CMP/GMP however BGP is recommended. BGP AS assignments for each national site are available in annex D appendixes.

Network Management

504. The CCCC will perform network management and monitoring using standard protocols (e.g. ICMP, SNMP). The CCCC will monitor inter-POP connectivity and the USA Blackbone. CMPs and GMPs may implement their own network management and monitoring tools within their own environments and uplinks. The CMPs/GMPs and CCCC will coordinate to enable visibility between environments; this may include the exchange of SNMP community strings or other details.

CHAPTER 6 - ENCLAVE NETWORK AND USER SERVICES

General

601. Each Enclave has at least the core services available. Services are divided in three groups. Core services, Core PLUS services and additional services. This is the CFBLNet default but CFBL will try to accommodate the customer request.

602. The core network services for the enclave are listed in Table D-6.1.

Ser **(a)**	**Information Service Description** **(b)**	**Status** **(c)**
1	IPv4 routing (BGP routing is default but others are possible)	Required
2	Encryption / decryption	Required
3	Network Time Protocol (NTP) Source	Required
4	Network management	Required

Table D-6.1, Enclave Core Network Services

603. The core PLUS network services for the enclave are listed in Table D-6.2. These services are available but are not in place by default.

Ser **(a)**	**Information Service Description** **(b)**	**Status** **(c)**
1	IPv6 routing	Available
2	Network Time Protocol (NTP) Source stratum 1	Available
3	Domain Name Service (DNS) server	Available
4	File Transfer Protocol (FTP) server	Available
5	Remote Authentication Dial In User Service (RADIUS) server	Available
6	Voice over IP call manager (VoIP)	Available
7	Broadcast <> multicast conversion	Available
8	Any cast	Available

Table D-6.2, Enclave Core PLUS Network Services

604. The additional network services for the enclave are listed in Table D-6.3.

Ser (a)	Information Service Description (b)	Status (c)
1	E-mail	Optional
	VTC server	Optional
2	WEB (http) server	Optional
3	WIKI server	Optional
4	Chat server	Optional
5	Active Directory (AD)	Optional
6	Lightweight Directory Access Protocol (LDAP)	Optional
7	MAP server	Optional
8	Collaborate server (like Adobe connect)	Optional
9	Update server	Optional
10	Ticket server (like OTRS)	Optional
11	Other service to be investigated as requested	Optional

Table D-6.3, Enclave additional user Services

Domain Name Service (DNS)

605. Each enclave supports a distributed DNS service with each CMP/GMP being responsible for managing its own DNS domains in accordance with the DNS naming convention as shown below.

Enclave-acronym.country-code

The enclave acronyms are provided in Appendix 2 of this document. The applicable country codes according the ISO 3 alpha standard are provided in Appendix 2 of this document.

606. Each enclave DNS is a federation of DNS servers, with the CCEB, NATO and USA providing the root DNS server. The master DNS root server is provided by the initiative lead group (CCEB, NATO or USA). Each CMP/GMP can have a national DNS top level domain server. In case the enclave is only between two countries the countries, one of the countries provide the master root server and the other could provide the slave root server

Electronic Mail (E-mail)

607. The enclave supports a distributed e-mail service between CMP/GMPs.

608. Simple Message Transfer Protocol (SMTP) is the agreed e-mail protocol between CMP/GMPs. CMP/GMPs may implement their own national e-mail protocols, ensuring they provide an SMTP interface at their national/organizational POP boundary.

609. In general, e-mail on the enclave is routed according to the DNS Mail Exchange (MX) record. Other (e.g. static) mail routing can be implemented as agreed between CMP/GMPs.

E-mail Account Naming Convention

610. Participant will establish e-mail accounts as either:
a. Permanent accounts for management or engineering purposes; or
b. Temporary accounts for each Initiative as required.

611. There are three types of accounts that can be used in the enclave to effect communications between users as listed in Table D-6.2.

Ser (a)	Account Type (b)	Example (c)
1	Personnel–normally used for enduring accounts (management, engineering etc)	bill.smith@, felicity.smith@
2	Organizational–normally used for operational/warfighter accounts	cflcc.g6@, asbde.s3@uk3cdobde.s2
3	Group–for address lists	CCCC.staff@, cflcc.staff@

Table D-6.2, Enclave E-mail Account Strategy

612. The recommended convention for enclave e-mail accounts is:

<first name>.<last name>@ <enclave>.<country>

Web Services

613. The enclave supports the Web service (HTTP and HTTPS) protocols to provide Web services across the enclave for management and engineering coordination as well as the delivery of Web-based information sources and products for initiatives.

614. CMP/GMPs are actively encouraged to populate these Web services in support of information dissemination for the purposes of CFBLNet management/coordination and to support Initiatives. CMP/GMPs should advise the NWG when a permanent or temporary Website is established in the enclave.

615. Should classified CFBL information need to be made available, a website will be stood up in the enclave.

Network Time Protocol (NTP)

616. Each enclave supports the Network Time Protocol (NTP) in order to provide a stable time source, synchronized across the wide area.

617. If a Stratum 1 time source is available then this is the primary NTP source for the enclave. National PoP routers are peered with each other. Other national/organisational sites will establish a one way server relationship with their nearest time source.

IP Telephony

618. Each enclave supports IP Telephony (VoIP) for in-band secure communications between the CMP/GMPs. It is also the primary means of secure communications for the CFBLNet management and engineering communities.

619. Each enclave site should have at least one VoIP (hardware or software phone) capability onsite as a minimum that is compatible with the enclave standard system. This phone is primarily for engineering management and coordination. Each site must coordinate with a “Call Manager-enabled” site to have its VoIP phone managed.

620. The Voice over IP (VoIP) Phone Numbers allocated for the enclaves are detailed in Pub 1 Annex C appendices.